What Is Claimed Is:

Sub A1

1. A method for providing content-based intrusion detection for a computer system by using an agile kernel-based auditing system, comprising:

receiving an audit specification;

wherein the audit specification specifies at least one target attribute to be recorded from a set of possible target attributes during an auditing process by the auditing system;

wherein the audit specification also specifies at least one auditing criterion that triggers recording of the at least one target attribute during the auditing process;

configuring the auditing system to record the at least one target attribute in response to detecting the at least one auditing criterion;

running the auditing system to produce an audit log by recording the at least one target attribute in response to detecting the at least one auditing criterion; and

examining the audit log to detect patterns for intrusion detection purposes.

2. The method of claim 1, further comprising:

detecting an event during the auditing process; and

in response to detecting the event, dynamically adjusting the auditing system during the auditing process to change the at least one auditing criterion and/or the at least one target attribute for subsequent operation of the auditing system.

3. The method of claim 1, wherein the auditing system is configured to modify a system call jump table to cause at least one selected system call to

execute code that causes the at least one target attribute to be recorded in response to detecting the at least one auditing criterion.

4. The method of claim 1, wherein the at least one target attribute can include:

an argument from a system call;

a parameter of a process making the system call;

data read during the system call;

data written during the system call;

a parameter of a file involved in the system call; and

a parameter relating to a network communication involved in the system call.

5. The method of claim 1, wherein configuring the auditing system to record the at least one target attribute involves:

compiling the audit specification to produce a kernel module;

loading the kernel module into a kernel of an operating system of the computer system; and

linking code from within the kernel module into system calls within the operating system.

6. The method of claim 1, wherein the at least one auditing criterion can include:

a user identifier for a process that is making a system call;

an identifier for an application program from which the system call is being made; and

an identifier for a file being accessed by the system call.

7. The method of claim 1, wherein producing the audit log involves filtering the at least one target attribute to reduce an amount of data stored in the audit log.

8. The method of claim 1, wherein producing the audit log involves:

determining at least one characteristic of the at least one target attribute; and

recording the at least one characteristic in the audit log.

9. The method of claim 1, wherein the audit specification is received from one of:

a user of the auditing system; and

an intrusion detection mechanism.

10. A computer-readable storage medium storing instructions that when executed by a computer cause the computer to perform a method for providing content-based intrusion detection for a computer system by using an agile kernel-based auditing system, the method comprising:

receiving an audit specification;

wherein the audit specification specifies at least one target attribute to be recorded from a set of possible target attributes during an auditing process by the auditing system;

wherein the audit specification also specifies at least one auditing criterion that triggers recording of the at least one target attribute during the auditing process;

configuring the auditing system to record the at least one target attribute in response to detecting the at least one auditing criterion in response to detecting the at least one auditing criterion;

running the auditing system to produce an audit log by recording the at least one target attribute; and

examining the audit log to detect patterns for intrusion detection purposes.

11. The computer-readable storage medium of claim 10, wherein the method further comprises:

detecting an event during the auditing process; and

in response to detecting the event, dynamically adjusting the auditing system during the auditing process to change the at least one auditing criterion and/or the at least one target attribute for subsequent operation of the auditing system.

12. The computer-readable storage medium of claim 10, wherein the auditing system is configured to modify a system call jump table to cause at least one selected system call to execute code that causes the at least one target attribute to be recorded in response to detecting the at least one auditing criterion.

13. The computer-readable storage medium of claim 10, wherein the at least one target attribute can include:

an argument from a system call;

a parameter of a process making the system call;

data read during the system call;

data written during the system call;

a parameter of a file involved in the system call; and

a parameter relating to a network communication involved in the system call.

14. The computer-readable storage medium of claim 10, wherein configuring the auditing system to record the at least one target attribute involves:

compiling the audit specification to produce a kernel module;

loading the kernel module into a kernel of an operating system of the computer system; and

linking code from within the kernel module into system calls within the operating system.

15. The computer-readable storage medium of claim 10, wherein the at least one auditing criterion can include:

a user identifier for a process that is making a system call;

an identifier for an application program from which the system call is being made; and

an identifier for a file being accessed by the system call.

16. The computer-readable storage medium of claim 10, wherein producing the audit log involves filtering the at least one target attribute to reduce an amount of data stored in the audit log.

17. The computer-readable storage medium of claim 10, wherein producing the audit log involves:

determining at least one characteristic of the at least one target attribute; and

recording the at least one characteristic in the audit log.

18. The computer-readable storage medium of claim 10, wherein the audit specification is received from one of:

a user of the auditing system; and

an intrusion detection mechanism.

19. A apparatus for providing content-based intrusion detection for a computer system by using an agile kernel-based auditing mechanism, comprising:

an auditing mechanism that is configured to audit system calls;

a receiving mechanism that is configured to receive an audit specification;

wherein the audit specification specifies at least one target attribute to be recorded from a set of possible target attributes during an auditing process by the auditing mechanism;

wherein the audit specification also specifies at least one auditing criterion that triggers recording of the at least one target attribute during the auditing process;

an initialization mechanism that configures the auditing mechanism to record the at least one target attribute in response to detecting the at least one auditing criterion;

wherein the auditing mechanism is configured to produce an audit log by recording the at least one target attribute in response to detecting the at least one auditing criterion; and

an intrusion detection mechanism that is configured to examine the audit log to detect patterns for intrusion detection purposes.

20. The apparatus of claim 19, wherein the initialization mechanism is further configured to:

detect an event during the auditing process; and

in response to detecting the event, to dynamically adjust the auditing mechanism during the auditing process to change the at least one auditing criterion and/or the at least one target attribute for subsequent operation of the auditing mechanism.

21. The apparatus of claim 19, wherein the auditing mechanism is configured to modify a system call jump table to cause at least one selected system call to execute code that causes the at least one target attribute to be recorded in response to detecting the at least one auditing criterion.

22. The apparatus of claim 19, wherein the at least one target attribute can include:

an argument from a system call;

a parameter of a process making the system call;

data read during the system call;

data written during the system call;

a parameter of a file involved in the system call; and

a parameter relating to a network communication involved in the system call.

23. The apparatus of claim 19, wherein the auditing mechanism is configured to:

compile the audit specification to produce a kernel module;

load the kernel module into a kernel of an operating system of the computer system; and to

link code from within the kernel module into system calls within the operating system.

24. The apparatus of claim 19, wherein the at least one auditing criterion can include:

a user identifier for a process that is making a system call;

an identifier for an application program from which the system call is being made; and

an identifier for a file being accessed by the system call.

25. The apparatus of claim 19, wherein the auditing mechanism is configured to produce the audit log by filtering the at least one target attribute to reduce an amount of data stored in the audit log.

26. The apparatus of claim 19, wherein the auditing mechanism is configured to produce the audit log by:

determining at least one characteristic of the at least one target attribute; and

recording the at least one characteristic in the audit log.

27. The apparatus of claim 19, wherein the audit specification is received from one of:

a user of the auditing mechanism; and

the intrusion detection mechanism.